aruba
a Hewlett Packard Enterprise company

Aruba 360 Secure Fabric

Protecting your data from the insider threat, Introducing the Aruba 360 Secure Mobile Fabric

Austin Hawthorne
Sr. Director, Aruba Security

TODAY'S EVOLVING SECURITY CHALLENGES

MOBILE, BYOD, CLOUD

VULNERABLE IOT

ATTACKS ON THE INSIDE

$3M	3M	$3T
Per Incident	Open Jobs	In Damage

aruba
a Hewlett Packard Enterprise company

Let’s talk about the insider threat….

COMPROMISED

40 million credit cards were stolen from Target’s severs

STOLEN CREDENTIALS

MALICIOUS

Edward Snowden stole more than 1.7 million classified documents

INTENDED TO LEAK INFORMATION

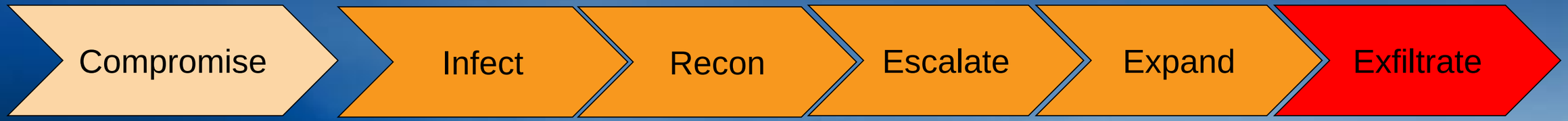
NEGLIGENT

Employees uploading sensitive information to personal Dropbox for easy access

DATA LEAKAGE

aruba
a Hewlett Packard Enterprise company

Anatomy of An Attack On the Inside - Credit Card Theft



Infect Sub-contractor

Upload Malware To Web Server

Understand Network Topology/AD

“Pass-The-Hash”

Install Malware On POS

Set up ftp Server

Traditional Security Paradigm

Trust but Verify

Zero Trust

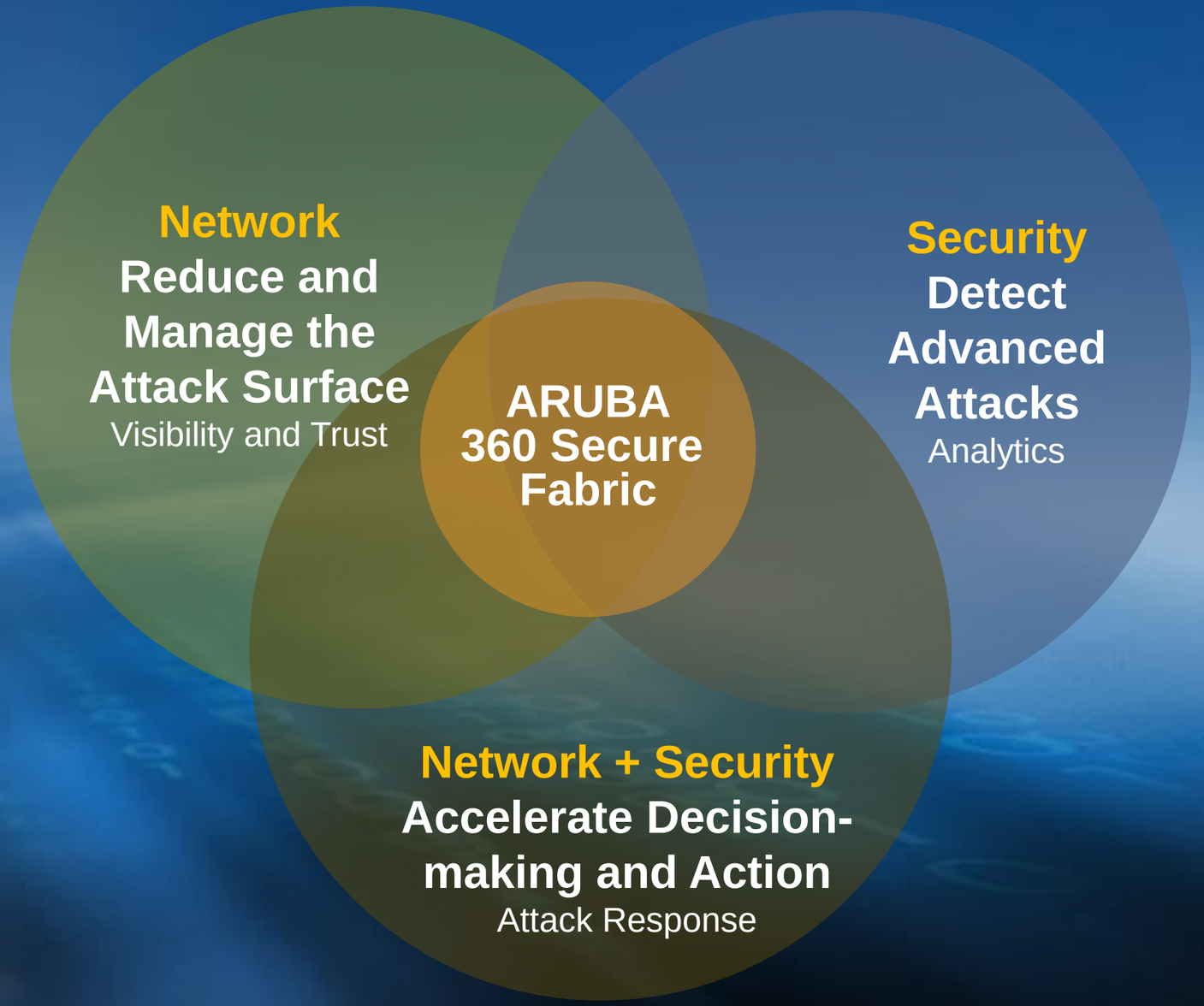
Never Trust, Always Verify

aruba
a Hewlett Packard Enterprise company

Aruba Security Vision

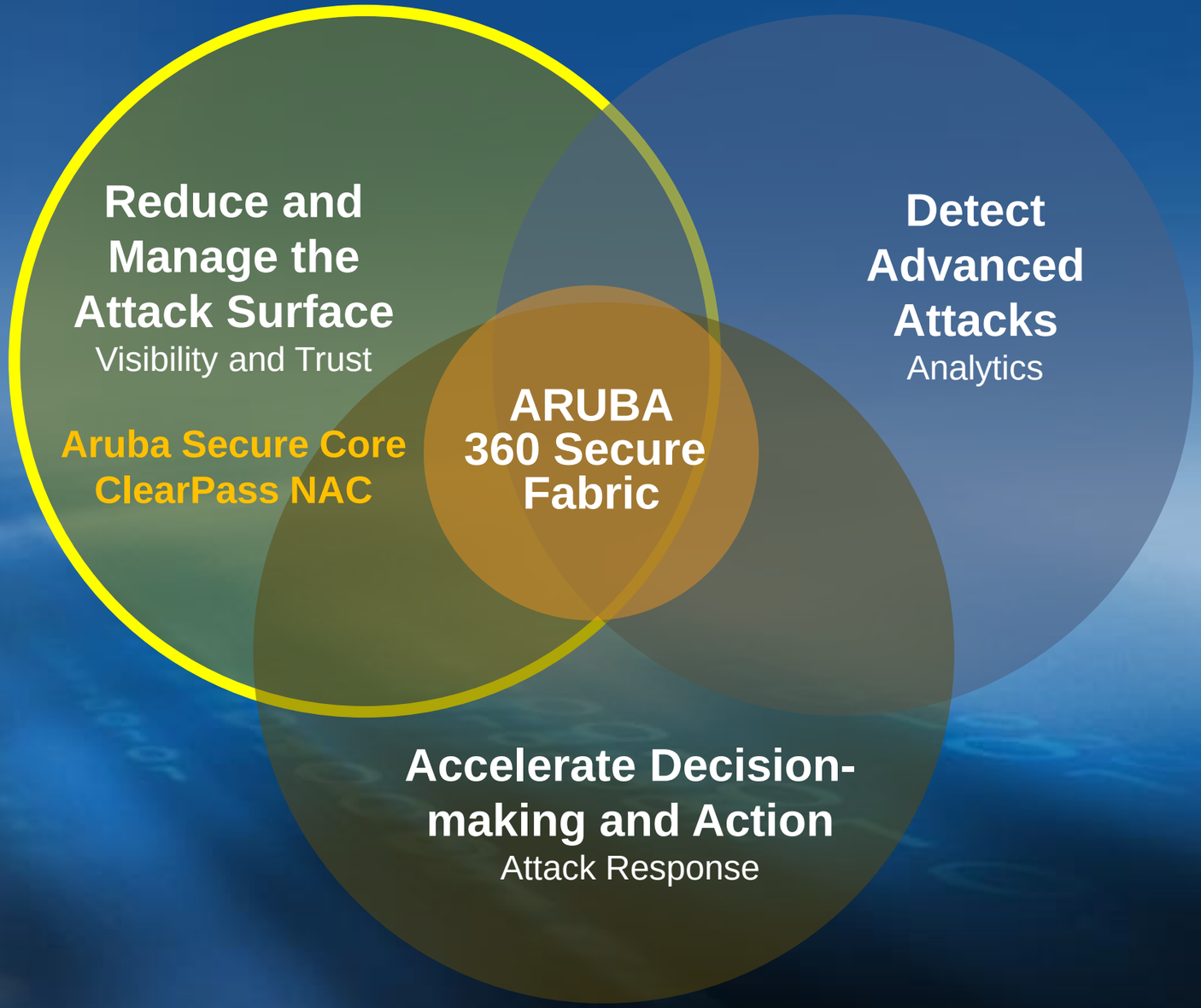
1. The network infrastructure and transport is trustworthy.
2. No anonymous network connections. Every device is identified using the most practical identification scheme available.
3. Identity leads to role. Role determines access rights. The network enforces principle of least privilege.
4. Security requires system-level, enterprise-wide coordination. Point products can’t do it alone.
5. The network sees the attacker (sensing).
6. Analytics detects the attack (sense-making).
7. The analyst has full visibility of all network activity which aids in (decision-making).
8. The network thwarts the attacker (action).

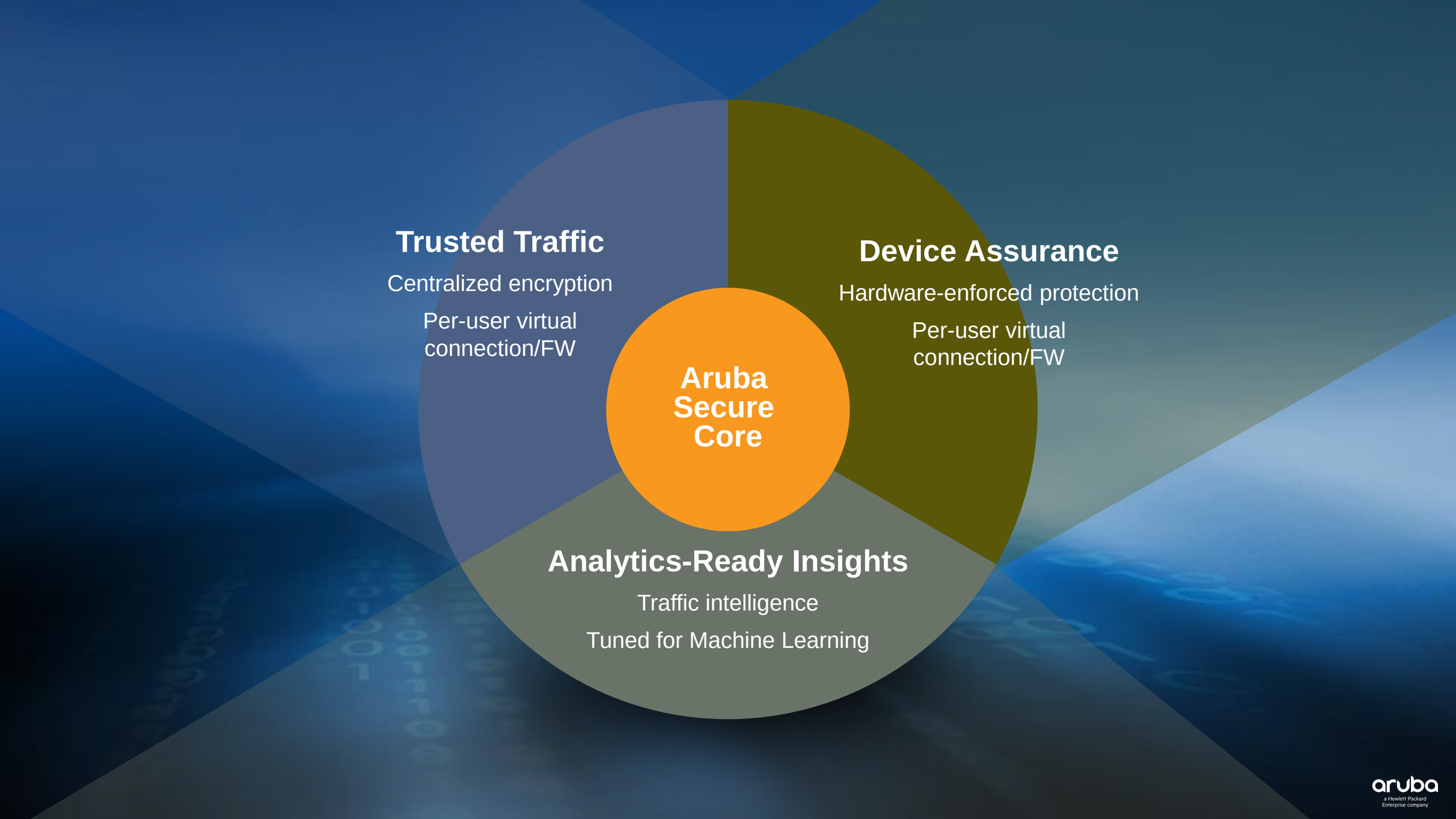
THE NEW SECURITY IMPERATIVE



aruba
a Hewlett Packard Enterprise company

THE NEW SECURITY IMPERATIVE





Intelligent traffic control with application visibility

On-Board DPI

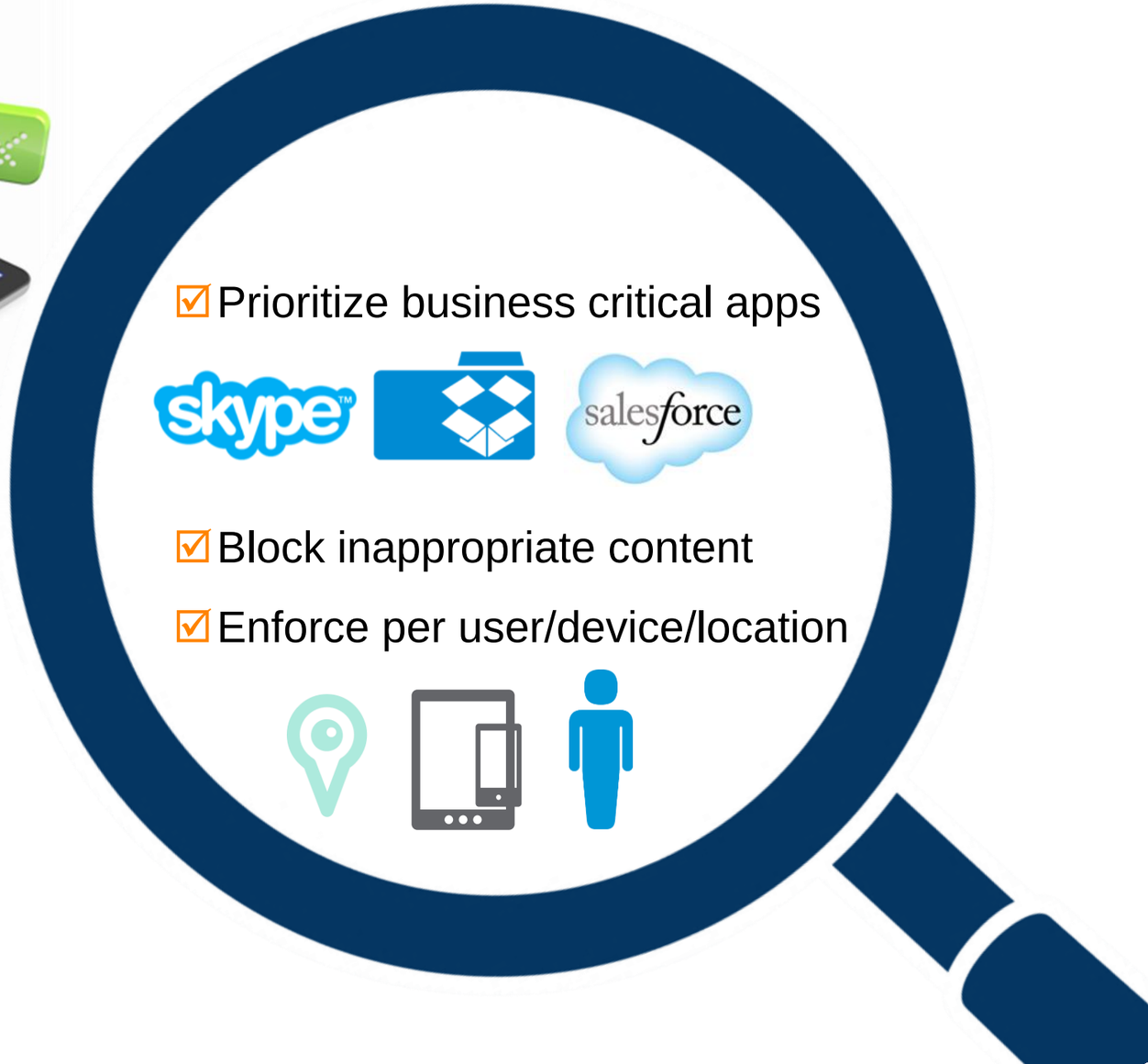
- Depth - common apps
- Enterprise traffic

Cloud-Based Web Policy Enforcement

- Breadth - less common apps
- Web traffic

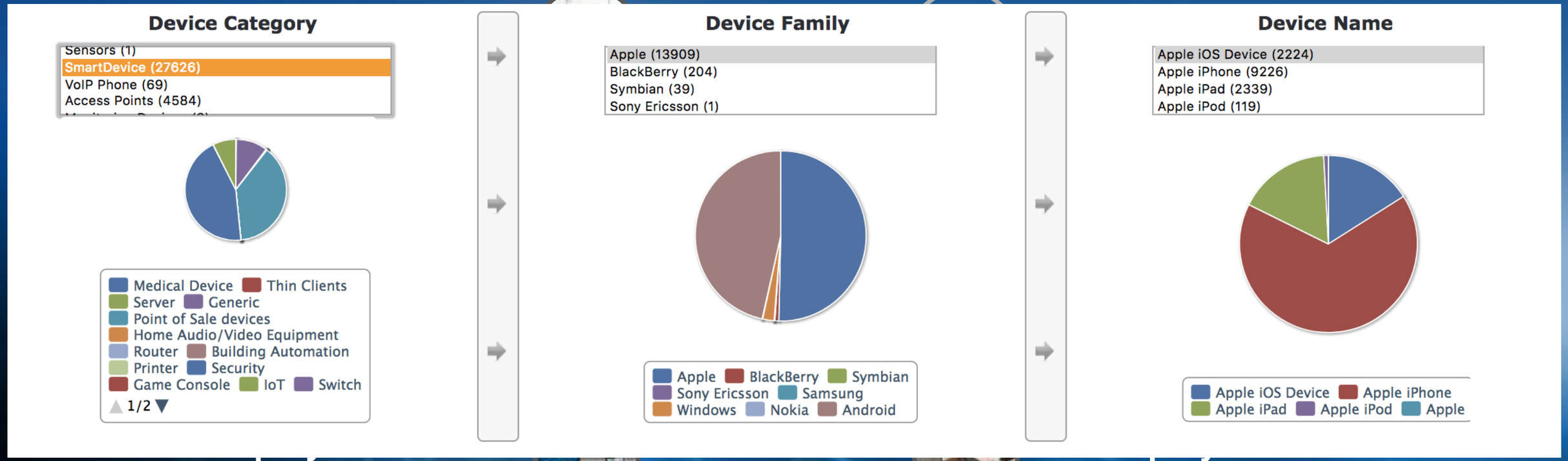
GRANULAR VISIBILITY & CONTROL

- ❑ App category
- ❑ Individual app
- ❑ Web category
- ❑ Web reputation
- ❑ Allow/deny
- ❑ QoS
- ❑ Throttle
- ❑ Log
- ❑ Blacklist



aruba
a Hewlett Packard Enterprise company

Visibility: What's On Your Network?



ClearPass Secure Network Access Control

Adaptive Policy Using Device Ownership

Enterprise Laptop

Authentication → EAP-TLS

SSID → CORP-SECURE

Internet and Intranet

BYOD Phone

Authentication → EAP-TLS

SSID → CORP-SECURE

Internet Only

Security/Context Automation and Orchestration

Who: **Bob**
Group: **Faculty**
Device: **Personal iPad**
Location: **Room 104**
Time: **9am, Monday**
Compliance: **Healthy**
Mac Address: X
IP Address: Y
Airgroup **Permissions**

Adaptive Trust Identity

WHO WHAT WHERE WHEN

CLEARPASS
ACCESS
MANAGEMENT

AD/LDAP — WHO

EMM/MDM — WHO WHAT WHRE WHEN

Update WLAN

Update Firewall

Update Web Proxy / Filter

Logon to Applications (SSO)

Update EMM/MDM

aruba
a Hewlett Packard Enterprise company

ClearPass Exchange: End to End Control

Internet of Things (IoT)

Multi-vendor switching

BYOD and corporate owned

Multi-vendor WLANs

Aruba ClearPass with Exchange Ecosystem

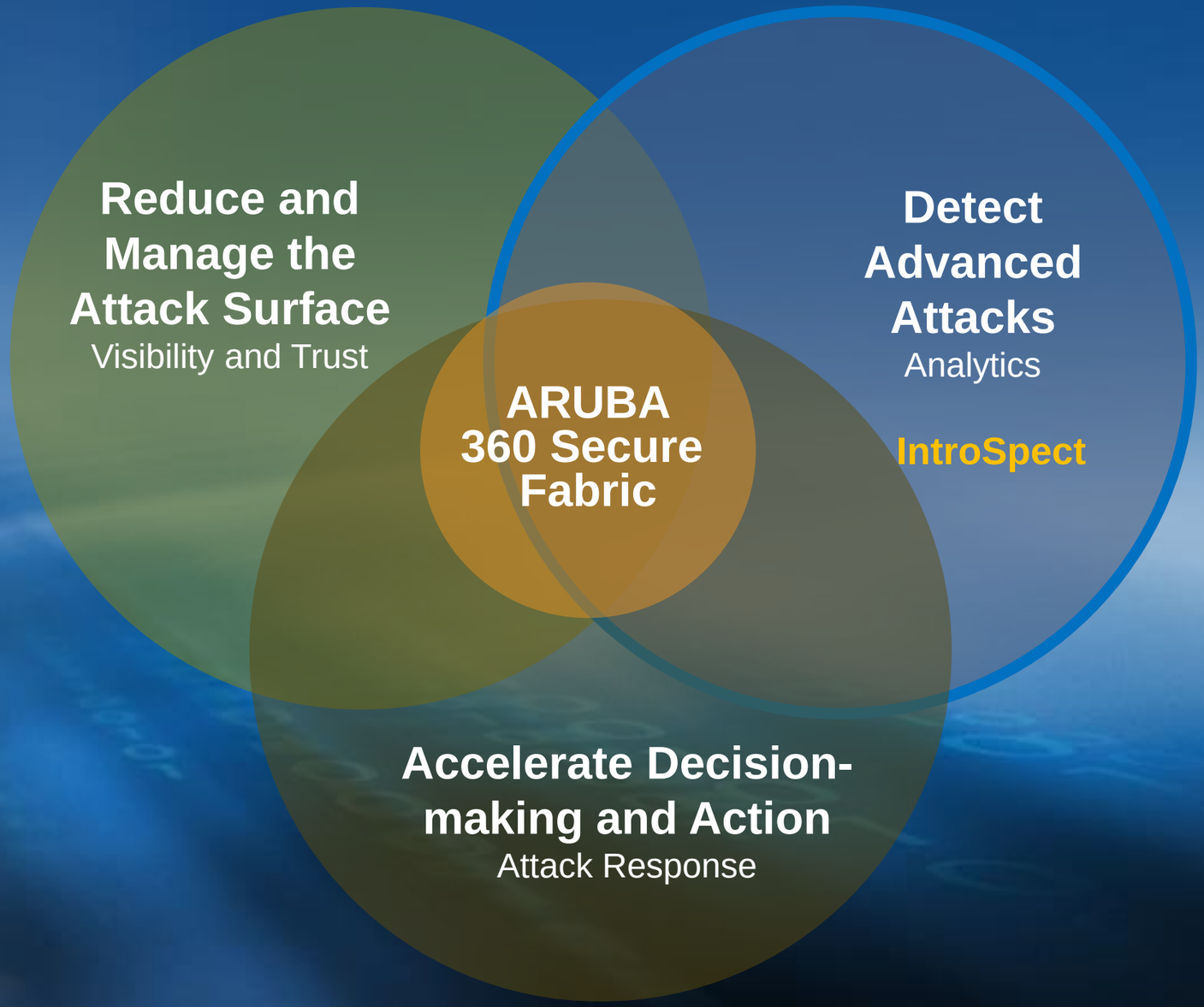
REST API, Syslog

Security monitoring and threat prevention

Device management and multi-factor authentication

Helpdesk and voice/SMS service in the cloud

THE NEW SECURITY IMPERATIVE

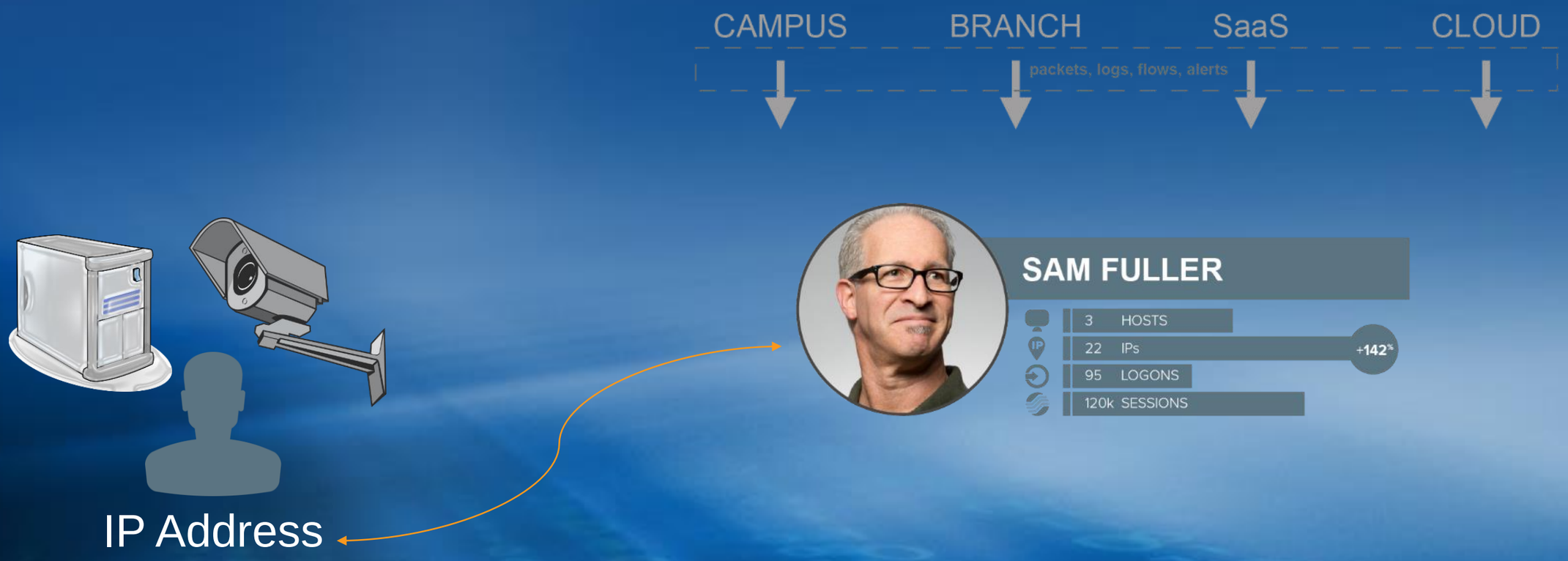


ATTACKS AND RISKY BEHAVIORS
on the inside

INTROSPECT FOCUSES ON TWO KEY SECURITY CHALLENGES

EFFICIENCY AND EFFECTIVENESS
of the security team

The Start: User/Entity View of Events



Behavior – Many Different Dimensions

Internal Resource Access
Finance servers

Authentication
AD logins

Remote Access
VPN logins

External Activity
C&C, personal email

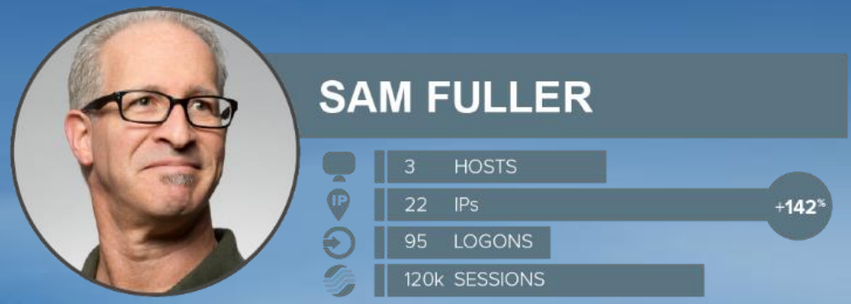
Behavioral Analytics

SaaS Activity
Office 365, Box

Cloud IaaS
AWS, Azure

Physical Access
badge logs

Exfiltration
DLP, Email



Behavioral Analytics—Finding Small Changes

MACHINE LEARNING

UNSUPERVISED

Behavioral Analytics

BASELINES

HISTORICAL

+

PEER GROUP

ABNORMAL INTERNAL RESOURCE ACCESS

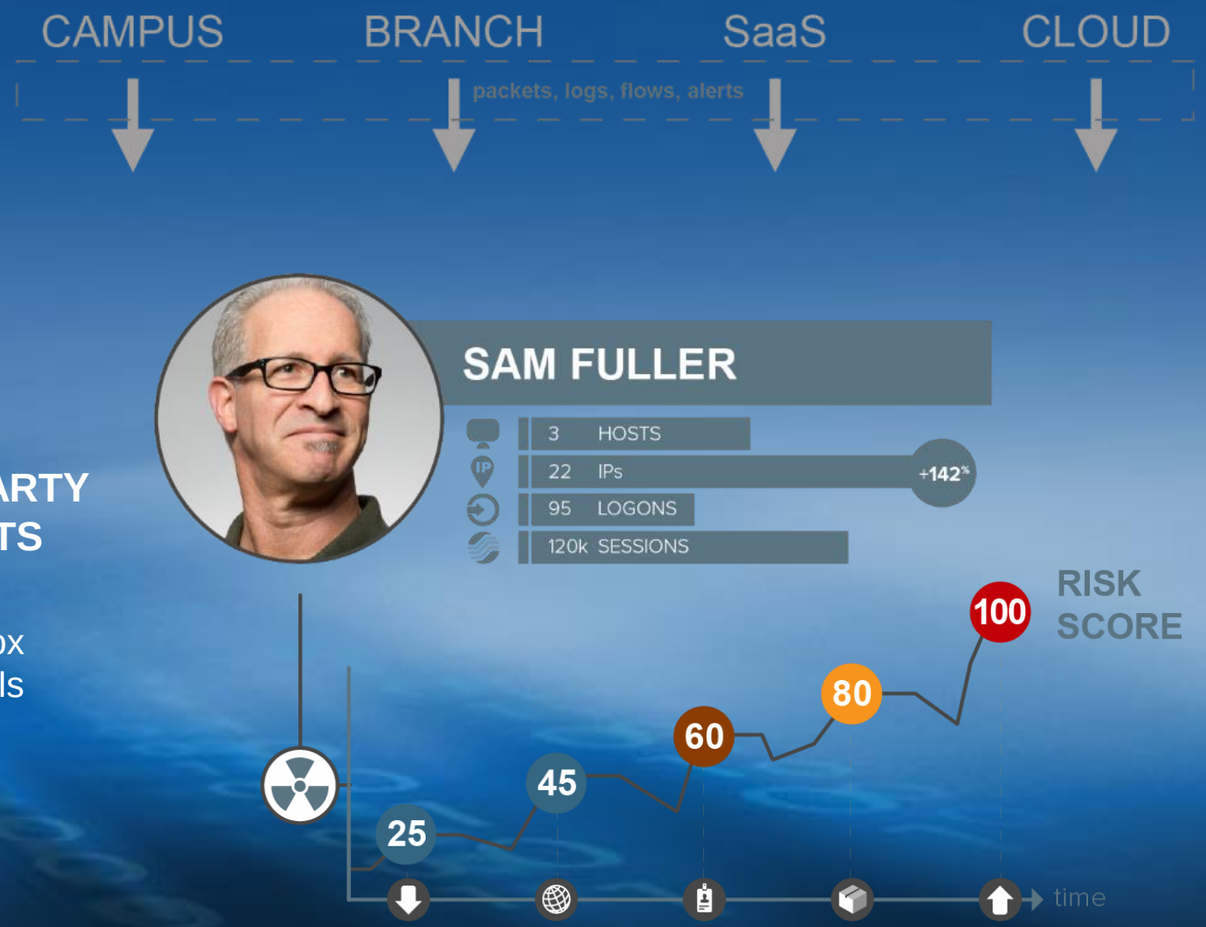
Peer Baseline Anomaly

Finding the Malicious in the Anomalous

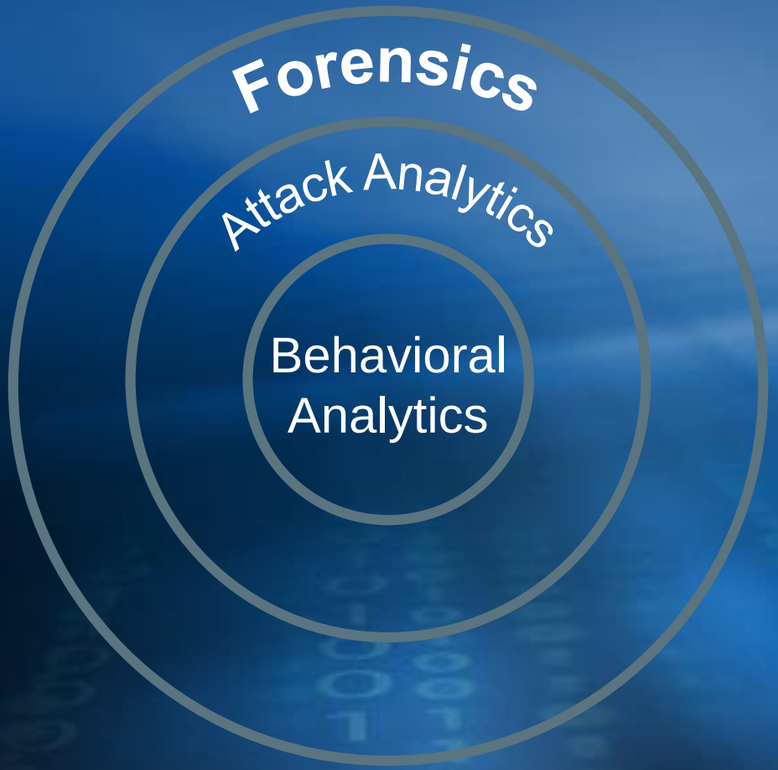
BUSINESS CONTEXT
High Value Assets
High Value Actors

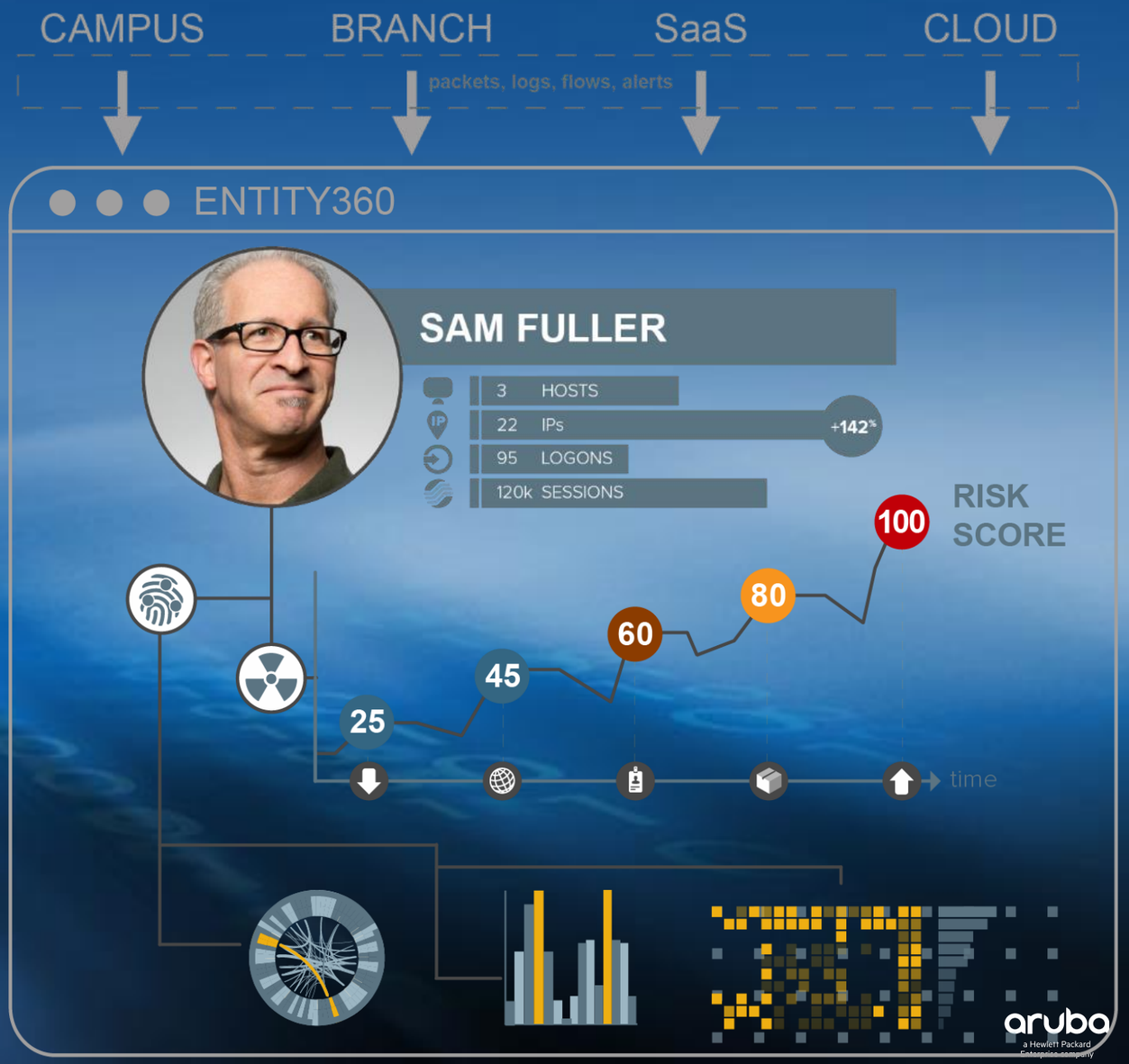
MACHINE LEARNING
SUPERVISED
UNSUPERVISED

THIRD PARTY ALERTS
DLP
Sandbox
Firewalls
STIX
Rules
Etc.



Accelerated Investigation and Response





INTROSPECT USE CASE: K-12 EDUCATION

PAIN POINTS

Initial: Inside Threat

During POC: Large amount of staff account lockouts but couldn't understand where or why

ARUBA SOLUTION

Fast detect and respond

Visibility and detection of threats not seen by their other security solutions

Threat hunting

User correlation

RESULTS WITH INTROSPECT

Within hours, IntroSpect detected where (single users PC) and why (Emotet banking trojan malware)

Isolated malware and prevented lateral movement and business interruption

Financial and student data protected

Root cause analysis and remediation within hours

Alerted neighboring districts to Emotet

ANOTHER SCHOOL DISTRICT WITHOUT INTROSPECT

Unable to correlate where and why account lockouts

Had to shut down ALL PCs to prevent lateral movement

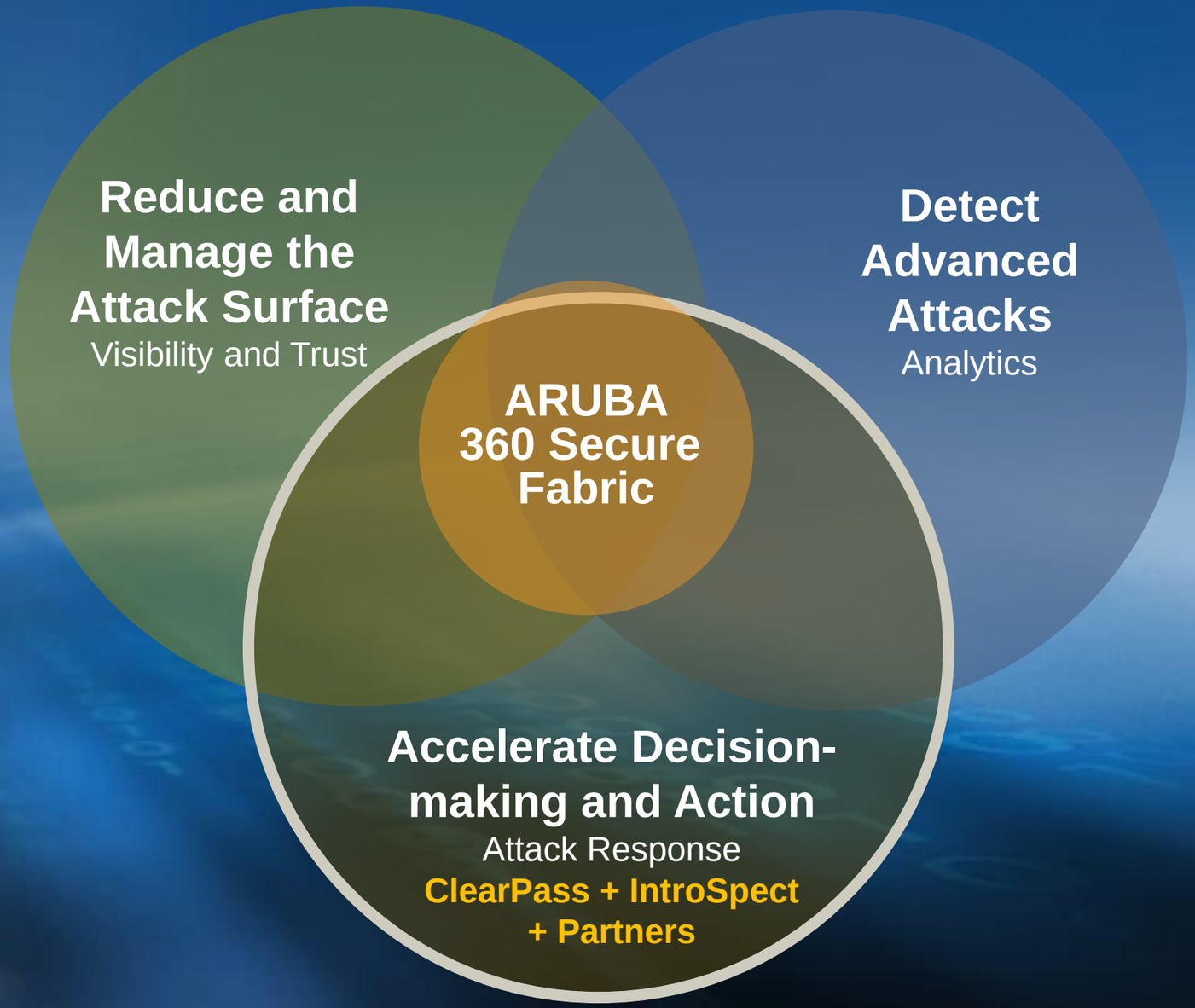
10 days later…virus was found

Due to lack of visibility, root cause analysis could not be completed

ALL machines in the ISD were reimaged

IT staff worked overnight 3 nights

THE NEW SECURITY IMPERATIVE



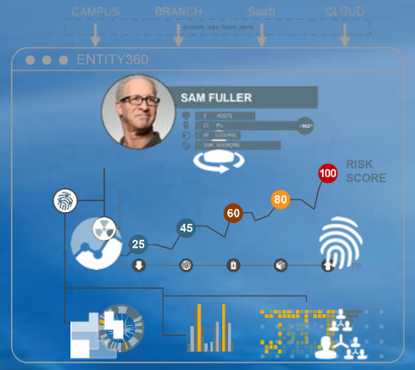
CLEARPASS + INTROSPECT = INTEGRATED PROTECTION

1. Discover and Authorize

User/Device Context

ClearPass
Secure Network Access Control

2. Monitor and Alert



Entity360 Profile with Risk Scoring

IntroSpect UEBA

Actionable Alerts

3. Decide and Act

- Real-time Quarantine
- Re-authentication
- Bandwidth Control
- Blacklist

ClearPass
Adaptive Response

aruba
a Hewlett Packard Enterprise company

CLEARPASS + PARTNERS = INTEGRATED PROTECTION

1. Discover and Authorize

User/Device Context

ClearPass
Secure Network Access Control

2. Monitor and Alert

McAfee™

paloalto NETWORKS

Radar

CARBON BLACK

aruba
a Hewlett Packard Enterprise company

IntroSpect or 360 Security Exchange Partners

Actionable Alerts

3. Decide and Act

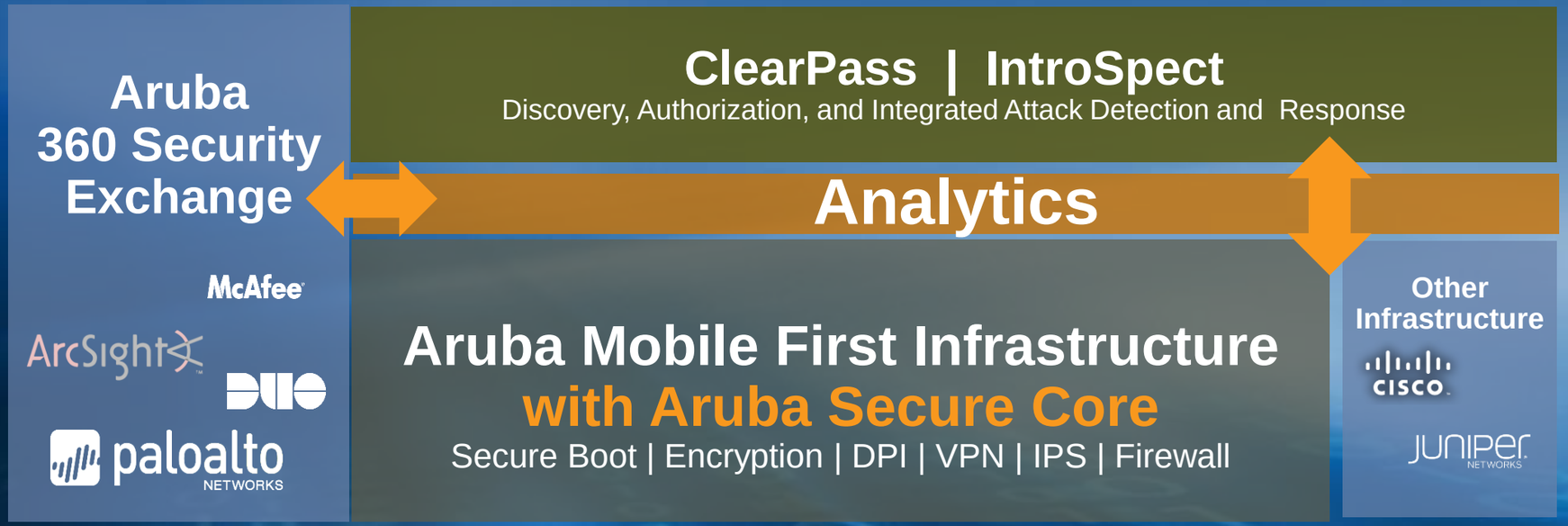
- Real-time Quarantine
- Re-authentication
- Bandwidth Control
- Blacklist

ClearPass
Adaptive Response

aruba
a Hewlett Packard Enterprise company

Analytics-Driven Active Cyber Protection

Aruba 360 Secure Fabric



aruba
a Hewlett Packard Enterprise company

aruba
a Hewlett Packard
Enterprise company